ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 512.6 10.23947/1992-5980-2017-17-1-122-131

Способ восстановления булевой функции нескольких переменных по ее производной*

А. В. Мазуренко[1], Н. С. Могилевская[2]**
[1,2] Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Method of restoring multivariable Boolean function from its derivative***

A. V. Mazurenko[1], N. S. Mogilevskaya[2]**
[1,2] Don State Technical University, Rostov-on-Don, Russian Federation

Введение. Булевы функции нескольких переменных играют важную роль в криптографии и теории кодирования. Композиции этих функций используются в ряде симметрических криптосистем; с их помощью могут быть определены некоторые помехоустойчивые коды, например, коды Рида-Маллера, коды Кердока, а также построены новые декодеры, работающие за пределом половины кодового расстояния. В работе рассматривается задача восстановления булевой функции по ее производной, названная задачей интегрирования булевых функций. При восстановлении булевой функции вектор, в направлении которого вычислена производная, полагается неизвестным.
Материалы и методы. Результаты получены на базе следующей методологии: теория булевых функций, теория конечных полей и полиномиальных колец, линейная алгебра. Пространство булевых функций рассмотрено как некоторое изоморфное факторкольцо, что позволило свести поставленную задачу к поиску решения полиномиальной системы уравнений специального вида. Построенный изоморфизм позволяет проверить, разрешима ли задача об интегрировании, а также предложить новый способ ее решения.
Результаты исследования. Формально построен алгоритм поиска прообраза методом полного перебора, вычислена его алгоритмическая сложность. Доказана теорема о необходимых и достаточных условиях существования прообраза для произвольной булевой функции, которая рассматривается как значение производной по направлению. Приводимые доказательства носят конструктивный характер. На основе доказанных фактов построены алгоритмы проверки существования прообраза для заданной булевой функции и построения прообраза. В предложенном варианте алгоритм строит только один из возможных прообразов, при условии его существования. Предложенный алгоритм построения прообраза обладает с точки зрения алгоритмической сложности значительной эффективностью по сравнению с методом полного перебора. Приводятся временные оценки сложности основных формальных алгоритмов, разработанных для решения поставленных задач, описано сравнение

Introduction. Boolean functions of several variables are of paramount importance in the coding theory and cryptography. The compositions of these functions are used in a set of the symmetric cryptosystems; therewith, some error-control codes, such as Reed-Muller codes, Kerdock codes, can be defined; as well as some new decoders operating beyond half of the code distance can be constructed. The task of restoring a Boolean function from its derivative which is called a Boolean function integration problem is considered. A Boolean function being restored, the vector towards which the derivative is calculated is supposed unknown.
Materials and Methods. The results are obtained on the basis of the following methodology: theory of Boolean functions, theory of finite fields and polynomial rings, linear algebra. The space of Boolean functions is considered a certain isomorphic factor-ring that allows reducing the task to finding solutions to a polynomial set of equations of a special form. The constructed isomorphism enables to check whether the integration problem is decidable, and also to offer a new method of its solution.
Research Results. The algorithm of searching preimage by the full enumeration method is formally constructed; and its algorithmic complexity is calculated. The theorem of necessary and sufficient conditions for the existence of an arbitrary Boolean function preimage regarded as the directional derivative value is proved. The provided proofs are constructive. On the basis of the established facts, the algorithms of checking the preimage existence for the specified Boolean function and of building the preimage are developed. In the proposed version, the algorithm forms only one of the possible preimages under the condition of its existence. The proposed algorithm of the preimage generation is significantly efficient from the standpoint of the algorithmic complexity compared to the full enumeration method. Time estimates of the complexity of the basic formal algorithms developed for solving the formulated problems are given. The comparison of their operation complexity to the algorithm of

* Работа выполнена в рамках инициативной НИР.
** E-mail: mazurencoal@gmail.com, 79044430127@yandex.ru
***The research is done within the frame of independent R&D.

сложности их работы со сложностью алгоритма интегрирования булевых функций методом полного перебора.
Обсуждение и заключения. Выполненная работа может быть полезна для специальных разделов криптографии и теории кодирования, в которых используются булевы функции нескольких переменных.

Boolean functions integration complexity by the complete enumeration method is described.
Discussion and Conclusions. The research performed can be useful for special sections of the coding theory and cryptography where Boolean functions of several variables are used.

Ключевые слова: булева функция, производная булевой функции по направлению, алгоритм проверки возможности восстановления булевой функции, оценка сложности, пространство булевых функций, кольцо многочленов, конечные поля, кольцевой изоморфизм, теория кодирования, поиск прообраза.

Keywords: Boolean function, directional derivative of Boolean function, algorithm of checking recoverability of Boolean function, complexity estimation, space of Boolean functions, polynomial ring, finite fields, ring isomorphism, coding theory, preimage searching.

Введение. Булевы функции нескольких переменных играют важную роль в криптографии и теории кодирования. Например, композиции этих функций используются в ряде симметрических криптосистем [1]; с их помощью могут быть определены, например, помехоустойчивые коды Рида-Маллера и коды Кердока [2, 3] и построены новые декодеры помехоустойчивых кодов, работающие за пределом половины кодового расстояния [3, 4, 5, 6]. Различные вопросы дифференциального исчисления булевых функций рассмотрены в [7, 8, 9]. В теории булевых функций естественным образом возникает понятие производной по направлению, представляющей собой оператор, действующий на пространстве булевых функций. Актуальной является задача исследования свойств данного оператора. В работе рассматривается задача восстановления булевой функции по ее производной по некоторому направлению, определены условия существования прообраза производной булевой функции, описан способ восстановления функции по ее прообразу и даны временные оценки сложности предложенных методов.

Формулировка задачи интегрирования булевых функций. Булевой функцией, согласно [1], назовем отображение $f: F_2^n \to F_2$, где F_2^n — векторное пространство размерности n над конечным полем F_2. Множество булевых функций от n переменных обозначим Φ_n. Известно, что $|\Phi_n| = 2^{2^n}$. Будем считать, что элементы множеств Φ_n и F_2^n упорядочены некоторым образом, например, лексикографически. Производной булевой функции $f(\overline{x})$ по направлению $\overline{u}$, где $\overline{u} \neq \overline{0}$, $\overline{u} \in F_2^n$, называется $(D_{\overline{u}} f)(\overline{x}) \in \Phi_n$:

$$(D_{\overline{u}} f)(\overline{x}) = f(\overline{x} + \overline{u}) + f(\overline{x}). \quad (1)$$

Функцию f назовем прообразом производной $D_{\overline{u}} f$.

Сформулируем задачу восстановления булевой функции по ее производной, которую далее будем называть задачей интегрирования. Дана булева функция $f \in \Phi_n$, необходимо найти хотя бы одну функцию $g \in \Phi_n$, такую, чтобы выполнялось равенство $f = D_{\overline{u}} g$ для некоторого $\overline{u} \neq \overline{0}$, $\overline{u} \in F_2^n$.

Необходимые предварительные сведения и результаты. В [1, стр. 69] сформулирована теорема, о том, что каждая функция $f \in \Phi_n$ может быть единственным образом представлена в виде полинома из кольца полиномов $F_2[x_1, x_2, ..., x_n]$, при этом степень полинома по каждой переменной не превосходит 1. Такое представление называется алгебраической нормальной формой (АНФ) булевой функции f.

Утверждение 1. Кольцо Φ_n изоморфно факторкольцу $F_2[x_1, x_2, ..., x_n]/I$, то есть $\Phi_n \cong F_2[x_1, x_2, ..., x_n]/I$, где $I = < x_1^2 + x_1, x_2^2 + x_2, ..., x_n^2 + x_n > \subset F_2[x_1, x_2, ..., x_n]$ — идеал в кольце $F_2[x_1, x_2, ..., x_n]$.

Утверждение 1 легко доказать, используя теорему из [1, стр. 69], и тот факт, что $F_2[x_1, x_2, ..., x_n]/I$ — факторкольцо, в котором представителями классов смежности являются полиномы, степень которых по каждой переменной не превосходит 1.

Пусть $[a]$ — класс смежности по модулю идеала I в кольце $F_2[x_1, x_2, ..., x_n]$. Тогда из утверждения 1 следует, что $[a]$ соответствует некоторой булевой функции $f \in \Phi_n$. Будем записывать булеву функцию $f \in \Phi_n$ в виде полинома, являющегося представителем класса смежности $[a]$:

$$f(x_1, x_2, ..., x_n) = a_0 + \sum_{i_1=1}^{n} a_{i_1} x_{i_1} + \sum_{1 \le i_1 < i_2 \le n} a_{i_1 i_2} x_{i_1} x_{i_2} + ... + \quad (2)$$
$$+ \sum_{1 \le i_1 < i_2 < ... < i_k \le n} a_{i_1 i_2 ... i_k} x_{i_1} x_{i_2} ... x_{i_k} + ... + a_{12...n} x_1 x_2 ... x_n.$$

Для f, заданной в виде (2) определим биективное отображение $\gamma: \Phi_n \to F_2^{2^n}$:

$$\gamma(f) = (a_0, a_1, ..., a_{12...n}) . \quad (3)$$

Обозначим S_A^k все возможные k-элементные подмножества множества A, где $k \in Z_{\geq 0}$.

По аналогии с k-м элементарным симметрическим многочленом [10] определим отображение

$$\sigma_k : F_2[x_1, x_2, ..., x_r, u_1, u_2, ..., u_v] \to F_2[x_1, x_2, ..., x_r, u_1, u_2, ..., u_v],$$

$$\sigma_k(x_1, x_2, ..., x_r, u_1, u_2, ..., u_v) = \sum_{\{y_1, y_2, ..., y_k\} \in S^k_{\{x_1, x_2, ..., x_r, u_1, u_2, ..., u_v\}}} y_1 y_2 ... y_k ,$$

где $k = \overline{1, r}$, r, $v \in N$. Положим, что $\sigma_0(\bar{x}, \bar{u}) = 1$, а при $k \notin \overline{1, r}$, $\sigma_k(\bar{x}, \bar{u}) = 0$.

Теорема 1 (об АНФ производной булевой функции). Для любого $f(\bar{x}) \in \Phi_n$ и $\bar{u} \neq \bar{0}$, $\bar{u} \in F_2^n$, справедливо

$$(D_{\bar{u}} f)(\bar{x}) = \sum_{k=1}^n \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} a_{i_1 i_2 ... i_k} [\sigma_k(x_{i_1}, x_{i_2}, ..., x_{i_k}, u_{i_1}, u_{i_2}, ..., u_{i_k}) + \quad (4)$$

$$+ x_{i_1} x_{i_2} ... x_{i_k} + \sum_{1 \leq j \leq k} x_{i_j} u_{i_j} \sigma_{k-2}(x_{i_1}, ..., x_{i_{j-1}}, x_{i_{j+1}}, ..., x_{i_k}, u_{i_1}, ..., u_{i_{j-1}}, u_{i_{j+1}}, ..., u_{i_k})],$$

где $(D_{\bar{u}} f)(\bar{x}) \in \Phi_n$.

Доказательство. Согласно (1) получаем

$$(D_{\bar{u}} f)(\bar{x}) = f(\bar{x} + \bar{u}) + f(\bar{x}) = f(x_1 + u_1, x_2 + u_2, ..., x_n + u_n) + f(x_1, x_2, ..., x_n) .$$

Из (2) следует, что

$$f(x_1 + u_1, x_2 + u_2, ..., x_n + u_n) = a_0 + \sum_{i_1=1}^n a_{i_1} \sigma_1(x_{i_1}, u_{i_1}) +$$

$$+ \sum_{1 \leq i_1 < i_2 \leq n} a_{i_1 i_2} (\sigma_2(x_{i_1}, x_{i_2}, u_{i_1}, u_{i_2}) + x_{i_1} u_{i_1} + x_{i_2} u_{i_2}) + ... +$$

$$+ \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} a_{i_1 i_2 ... i_k} [\sigma_k(x_{i_1}, x_{i_2}, ..., x_{i_k}, u_{i_1}, u_{i_2}, ..., u_{i_k}) +$$

$$\sum_{1 \leq j \leq k} x_{i_j} u_{i_j} \sigma_{k-2}(x_{i_1}, ..., x_{i_{j-1}}, x_{i_{j+1}}, ..., x_{i_k}, u_{i_1}, ..., u_{i_{j-1}}, u_{i_{j+1}}, ..., u_{i_k})] + ... +$$

$$+ a_{12...n} [\sigma_n(x_1, x_2, ..., x_n, u_1, u_2, ..., u_n) + \sum_{1 \leq j \leq n} x_j u_j \sigma_{n-2}(x_1, ..., x_{j-1}, x_{j+1}, ..., x_n, u_1, ..., u_{j-1}, u_{j+1}, ..., u_n)] .$$

Суммируя полученное выражение с $f(x_1, x_2, ..., x_n)$, доказываем (4). •

Установление связи коэффициентов исходной булевой функции и ее производной по направлению.

Пусть $[m..n] = \begin{cases} \{x \in N \mid m \leq x \leq n\}, m \leq n \\ \varnothing, n < m \end{cases}$, где m, $n \in N$, N — множество натуральных чисел. Обозначим через 2^A множество всех подмножеств множества A. Пусть

$$C_{[m,,n]} = \{i_1 ... i_k \mid i_j \in [m..n], i_1 < ... < i_k, k = \overline{m, n}, j = \overrightarrow{1, k}\} \subset N . \quad (5)$$

Обозначим для удобства $C_{[0..n]} = \{0\} \cup C_{[1..n]}$. Заметим, что $C_{[0..n]} \subset Z_{\geq 0}$, где $Z_{\geq 0}$ — множество целых неотрицательных чисел. Тогда, очевидным образом, можно упорядочить множество $C_{[0..n]}$, используя естественное упорядочение на множестве $Z_{\geq 0}$. Пусть

$$\lambda : C_{[0..n]} \to N \quad (6)$$

сопоставляет элементу $C_{[0..n]}$ его порядковый номер согласно введенному упорядочению (5). Очевидно, что λ является инъективным отображением.

Определим отображение $\tau : 2^{[1..n]} \to C_{[1..n]}$,

$$\tau(\{i_1, i_2, ..., i_k\}) = i_{j_1} i_{j_2} ... i_{j_k} , \quad (7)$$

где $\{i_1, i_2, ..., i_k\} = \{i_{j_1}, i_{j_2}, ..., i_{j_k}\}$; $i_{j_1} < i_{j_2} < ... < i_{j_k}$. Очевидно, что τ — биекция.

Пусть $f \in \Phi_n$ задана формулой (2), а $(D_{\bar{u}} f)(\bar{x})$ представлена формулой (4). Упорядочим мономы $(D_{\bar{u}} f)(\bar{x})$ по степеням переменных x_1, x_2, …, x_n:

$$(D_{\bar{u}} f)(\bar{x}) = [\sum_{i_1=1}^n a_{i_1} u_{i_1} + \sum_{1 \leq i_1 < i_2 \leq n} a_{i_1 i_2} u_{i_1} u_{i_2} + ... + \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} a_{i_1 i_2 ... i_k} u_{i_1} u_{i_2} .. u_{i_k} + ... +$$

$$+ a_{12...n} u_1 u_2 ... u_n] + \sum_{j_1=1}^n [\sum_{i_1 \in [1..n] \setminus \{j_1\}} a_{\tau(\{j_1, i_1\})} u_{i_1} + \sum_{\substack{i_1, i_2 \in [1..n] \setminus \{j_1\}, \\ i_1 < i_2}} a_{\tau(\{j_1, i_1, i_2\})} u_{i_1} u_{i_2} + ... +$$

$$\sum_{\substack{i_1, i_2, ..., i_{k-1} \in [1..n] \setminus \{j_1\}, \\ i_1 < i_2 < ... < i_{k-1}}} a_{\tau(\{j_1, i_1, ..., i_{k-1}\})} u_{i_1} u_{i_2} ... u_{i_{k-1}} + ... + a_{12...n} u_1 u_2 ... u_{j_1 - 1} u_{j_1 + 1} ... u_n] x_{j_1} + ... +$$

$$+ \sum_{\{j_1, j_2, ..., j_l\} \in S^l_{[1..n]}} [\sum_{i_1 \in [1..n] \setminus \{j_1, j_2, ... j_l\}} a_{\tau(\{j_1, j_2, ..., j_l, i_1\})} u_{i_1} + \sum_{\substack{i_1, i_2 \in [1..n] \setminus \{j_1, j_2, ... j_l\}, \\ i_1 < i_2}} a_{\tau(\{j_1, j_2, ..., j_l, i_1, i_2\})} u_{i_1} u_{i_2} + ... +$$

$$+\sum_{\substack{i_1,i_2,\ldots,i_{k-l}\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\},\\ i_1<i_2<\ldots<i_{k-l}}} a_{\tau(\{j_1,j_2,\ldots,j_l,i_1,\ldots,i_{k-l}\})}u_{i_1}u_{i_2}\ldots u_{i_{k-l}} +\ldots+ +a_{12\ldots n}\prod_{j\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\}} u_j\,]x_{j_1}x_{j_2}\ldots x_{j_l} +\ldots+$$

$$+\sum_{\{j_1,j_2,\ldots,j_{n-1}\}\in S^{n-1}_{[1..n]}} \sum_{i_1\in[1..n]\setminus\{j_1,j_2,\ldots,j_{n-1}\}} a_{\tau(\{j_1,j_2,\ldots,j_{n-1},i_1\})}u_{i_1}x_{j_1}x_{j_2}\ldots x_{j_{n-1}} .$$

Согласно теореме 1 $(D_{\overline{u}} f)(\overline{x})$ может быть представлена в виде:

$$(D_{\overline{u}} f)(\overline{x}) = b_0 + \sum_{i_1=1}^{n} b_{i_1}x_{i_1} + \sum_{1\le i_1<i_2\le n} b_{i_1i_2}x_{i_1}x_{i_2} +\ldots+$$

$$\sum_{1\le i_1<i_2<\ldots<i_k\le n} b_{i_1i_2\ldots i_k}x_{i_1}x_{i_2}\ldots x_{i_k} +\ldots+ b_{12\ldots n}x_1x_2\ldots x_n .$$

Сравним коэффициенты при соответствующих мономах и получим полиномиальную систему, состоящую из уравнений вида:

$$\sum_{i_1\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\}} a_{\tau(\{j_1,j_2,\ldots,j_l,i_1\})}u_{i_1} +\ldots+ \sum_{\substack{i_1,i_2\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\},\\ i_1<i_2}} a_{\tau(\{j_1,j_2,\ldots,j_l,i_1,i_2\}}u_{i_1}u_{i_2} +\ldots+ \quad (8)$$

$$+\sum_{\substack{i_1,i_2,\ldots,i_{k-l}\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\},\\ i_1<i_2<\ldots<i_{k-l}}} a_{\tau(\{j_1,j_2,\ldots,j_l,i_1,\ldots,i_{k-l}\}}u_{i_1}u_{i_2}\ldots u_{i_{k-l}} +\ldots+$$

$$+a_{12\ldots n}\prod_{j\in[1..n]\setminus\{j_1,j_2,\ldots,j_l\}} u_j = b_{j_1j_2\ldots j_l} ,$$

где $\{j_1, j_2,\ldots, j_l\}\subset 2^{[1..n]}$. Пусть $\varnothing\subset 2^{[1..n]}$ соответствует b_0. Очевидно, что $b_{12\ldots n}=0$. Таким образом, система, состоящая из уравнений (8), связывает коэффициенты исходной булевой функции и ее производной по направлению.

Пример. Рассмотрим Φ_2. Тогда система уравнений (8) принимает вид:

$$\begin{cases} a_1u_1 + a_2u_2 + a_{12}u_1u_2 = b_0, \\ a_{12}u_2 = b_1, \\ a_{12}u_1 = b_2, \\ 0 = b_{12}. \end{cases}$$

Рассмотрим Φ_3. Тогда система уравнений (8) принимает вид:

$$\begin{cases} a_1u_1 + a_2u_2 + a_3u_3 + a_{12}u_1u_2 + a_{13}u_1u_3 + a_{23}u_2u_3 + a_{123}u_1u_2u_3 = b_0, \\ a_{12}u_2 + a_{13}u_3 + a_{123}u_2u_3 = b_1, \\ a_{12}u_1 + a_{23}u_3 + a_{123}u_1u_3 = b_2, \\ a_{13}u_1 + a_{23}u_2 + a_{123}u_1u_2 = b_3, \\ a_{123}u_3 = b_{12}, \\ a_{123}u_2 = b_{13}, \\ a_{123}u_1 = b_{23}, \\ 0 = b_{123}. \end{cases}$$

Далее матрицу системы уравнений вида (8) относительно коэффициентов a_i обозначим $A\in M_{2^n\times(2^n-1)}(F_2)$. Расширенную матрицу системы обозначим через $A'\in M_{2^n\times 2^n}(F_2)$. Определим условия совместности системы из уравнений вида (8) при любом фиксированном $\overline{u}=(u_1,u_2,\ldots,u_n)\in F_2^n$. Из теоремы Кронекера-Капелли [10] известно, что СЛАУ совместна тогда и только тогда, когда ранг матрицы системы равен рангу расширенной матрицы. Следовательно, необходимо выбрать подходящие значения коэффициентов b_i в (8), чтобы $rank(A) = rank(A')$. Далее, определив значения b_i и a_j, построим булеву функцию g и вектор $\overline{y}$: $D_{\overline{y}}g = D_{\overline{u}}f$. Согласно определению производной по направлению из рассмотрения можно исключить случай, когда $\overline{u}=\overline{0}$.

Построение множества векторов, имеющих прообразы. Элементы векторного пространства $F_2^{2^n}$, взаимно однозначно соответствующие булевым функциям пространства Φ_n, для которых существует прообраз, назовем «разрешёнными». Множество «разрешённых» векторов обозначим $Allowed = \{\overline{y}\in F_2^{2^n} \mid \exists f\in\Phi_n, \overline{u}\ne\overline{0}\in F_2^n : D_{\overline{u}}f = \gamma^{-1}(\overline{y})\}$, где γ — биекция (3). Множество «запрещенных» векторов пространства булевых функций Φ_n обозначим $NotAllowed = F_2^{2^n}\setminus Allowed$. Очевидно, что $\Phi_n = Allowed \cup NotAllowed$, $Allowed \cap NotAllowed = \varnothing$.

Построим множества разрешенных и запрещенных векторов для Φ_1: $Allowed = \{(0,0),(1,0)\}$, $NotAllowed = \{(0,1),(1,1)\}$. Действительно,

$$(D_{(u_1)}f)(x_1) = a_0 + a_1(x_1+u_1) + a_0 + a_1x_1 = a_1u_1 .$$

Положим, что $n > 1$. Будем последовательно строить множество «разрешённых» векторов пространства булевых функций Φ_n. Построим «разрешённые» векторы при $\bar{u} = (1,0,...,0)$. Тогда система, состоящая из уравнений (8), содержит следующие уравнения:

$$a_1 = b_0\,,$$

$$0 = b_1\,,$$

$$a_{1 j_1 \dots j_k} = b_{j_1 \dots j_k}\,,$$

$$0 = b_{1 j_1 \dots j_k}\,,$$

где $2 \le j_1 < ... < j_k \le n$, $1 \le k \le n-1$. Таким образом, при $\bar{u} = (1,0,...,0)$ множество «разрешённых» векторов A_1, состоит из $\bar{y} \in F_2^{2^n}$: $\forall \{j_1,..., j_k\} \subset 2^{[1..n]\setminus\{1\}}$, где $1 \le k \le n-1$,

$$y_{\lambda(\tau(\{1, j_1,..., j_k\}))} = 0\,,$$

где λ определено формулой (6), τ — формулой (7).

При $\bar{u} = (0,...,0,1_i,0,...,0)$, где $i = \overline{1,n}$, множество «разрешённых» векторов A_i, состоит из $\bar{y} \in F_2^{2^n}$: $\forall \{j_1,..., j_k\} \subset 2^{[1..n]\setminus\{i\}}$, где $1 \le k \le n-1$,

$$y_{\lambda(\tau(\{i, j_1,..., j_k\}))} = 0\,.$$

Рассмотрим теперь вектор $\bar{u}$, который имеет l ненулевых координат u_{i_1}, u_{i_2}, … , u_{i_l}, где $1 \le i_1 < i_2 < ... < i_l \le n$, $1 \le l \le n$. Положим, что $I = \{i_1, i_2,..., i_l\}$. Тогда из системы уравнений вида (8) после подстановки такого $\bar{u}$ получаем систему, которая будет состоять из уравнений следующего вида:

$$\textstyle\sum_{k=1}^{l} \sum_{\{j_1, j_2,..., j_k\} \subset S_I^k} a_{\tau(\{j_1,..., j_k\})} = b_0\,, \tag{9.1}$$

$$\textstyle\sum_{k=1}^{l-h} \sum_{\{j_1, j_2,..., j_k\} \subset S^k_{I\setminus\{i_1', i_2',..., i_h'\}}} a_{\tau(\{i_1', i_2',..., i_h', j_1, j_2,..., j_k\})} = b_{\tau(\{i_1', i_2',..., i_h'\})}\,, \tag{9.2}$$

$$0 = b_{\tau(\{i_1, i_2,..., i_l, j_1', j_2',..., j_h'\})}\,, \tag{9.3}$$

$$\textstyle\sum_{k=1}^{l-d} \sum_{\{j_1, j_2,..., j_k\} \subset S^k_{I\setminus\{i_1', i_2',..., i_d'\}}} a_{\tau(\{i_1', i_2',..., i_d', j_1', j_2',..., j_v', j_1, j_2,..., j_k\})} = b_{\tau(\{i_1', i_2',..., i_d', j_1', j_2',..., j_v'\})}\,, \tag{9.4}$$

где $\{i_1', i_2',..., i_h'\} \subset 2^I$, $h = \overline{1, l-1}$; $\{j_1', j_2',..., j_h'\} \subset 2^{[1..n]\setminus I}$, $h = \overline{1, n-l}$; $\{i_1', i_2',..., i_d'\} \subset \bigcup_{d=0}^{l-1} S_I^d$, $\{j_1', j_2',..., j_v'\} \subset 2^{[1..n]\setminus I}$, $v = \overline{1, n-l}$.

Строка матрицы A системы уравнений вида (8), соответствующая уравнению вида (9.1), является линейно независимой относительно остальных строк матрицы. Строки, соответствующие уравнениям вида (9.3), являются нулевыми. Выделим среди строк матрицы A, соответствующих уравнениям вида (9.2), линейно зависимые. Для линейной зависимости двух векторов, соответствующие уравнениям вида (9.2), необходимо и достаточно, чтобы в левой части уравнения стояли одинаковые неизвестные. Следовательно, для таких уравнений число фиксированных координат, фигурирующих при индексе свободных членов, должно быть одинаково.

Рассмотрим два уравнения, соответствующие линейно зависимым строкам:

$$\textstyle\sum_{k=1}^{l-h} \sum_{\{j_1^{(1)}, j_2^{(1)},..., j_k^{(1)}\} \subset S^k_{I\setminus\{i_1^{(1)}, i_2^{(1)},..., i_h^{(1)}\}}} a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(1)}, i_{z+2}^{(1)},..., i_h^{(1)}, j_1^{(1)}, j_2^{(1)},..., j_k^{(1)}\})} = b_{\tau(\{i_1^{(1)}, i_2^{(1)},..., i_h^{(1)}\})}\,,$$

$$\textstyle\sum_{k=1}^{l-h} \sum_{\{j_1^{(2)}, j_2^{(2)},..., j_k^{(2)}\} \subset S^k_{I\setminus\{i_1^{(2)}, i_2^{(2)},..., i_h^{(2)}\}}} a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(2)}, i_{z+2}^{(2)},..., i_h^{(2)}, j_1^{(2)}, j_2^{(2)},..., j_k^{(2)}\})} = b_{\tau(\{i_1^{(2)}, i_2^{(2)},..., i_h^{(2)}\})}\,,$$

где $\{i_1, i_2,..., i_z\} = \{i_1^{(1)}, i_2^{(1)},..., i_h^{(1)}\} \cap \{i_1^{(2)}, i_2^{(2)},..., i_h^{(2)}\}$, $\{i_{z+1}^{(1)}, i_{z+2}^{(1)},..., i_h^{(1)}\} = \{i_1^{(1)}, i_2^{(1)},..., i_h^{(1)}\} \setminus \{i_1^{(2)}, i_2^{(2)},..., i_h^{(2)}\} \ne \varnothing$, $\{i_{z+1}^{(2)}, i_{z+2}^{(2)},..., i_h^{(2)}\} = \{i_1^{(2)}, i_2^{(2)},..., i_h^{(2)}\} \setminus \{i_1^{(1)}, i_2^{(1)},..., i_h^{(1)}\} \ne \varnothing$,

l — число ненулевых координат в $\bar{u}$. Легко увидеть, что

$$a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(1)}, i_{z+2}^{(1)},..., i_h^{(1)}, j_1^{(1)}\})} = a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(2)}, i_{z+2}^{(2)},..., i_h^{(2)}, j_1^{(2)}\})} \Leftrightarrow$$

$$\Leftrightarrow j_1^{(1)} \in \{i_{z+1}^{(2)}, i_{z+2}^{(2)},..., i_h^{(2)}\}\,,\ j_1^{(2)} \in \{i_{z+1}^{(1)}, i_{z+2}^{(1)},..., i_h^{(1)}\}\,,\ h = z+1\,.$$

Таким образом, равенства преобразуются к виду

$$a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(1)}, i_{z+1}^{(2)}\})} = a_{\tau(\{i_1, i_2,..., i_z, i_{z+1}^{(2)}, i_{z+1}^{(1)}\})}\,.$$

Следовательно, в силу произвольности выбора элементов $j_1^{(1)}$ и $j_1^{(2)}$, $h = l-1$. Таким образом, для того чтобы два вектора из матрицы A, соответствующих уравнениям вида (9.2), со свободными членами равными $b_{\tau(\{i_1^{(1)},i_2^{(1)},...,i_h^{(1)}\})}$ и $b_{\tau(\{i_1^{(2)},i_2^{(2)},...,i_h^{(2)}\})}$ были линейно зависимы необходимо и достаточно, чтобы выполнялись условия

$$h = l-1,$$

$$\{i_1^{(1)},i_2^{(1)},...,i_h^{(1)}\}\Delta\{i_1^{(2)},i_2^{(2)},...,i_h^{(2)}\} = \{i,j\},$$

где $I\setminus\{i_1^{(1)},i_2^{(1)},...,i_h^{(1)}\} = \{i\}$, $I\setminus\{i_1^{(2)},i_2^{(2)},...,i_h^{(2)}\} = \{j\}$, а знак «$\Delta$» обозначает симметрическую разность множеств.

Положим теперь, что в матрице A найдутся три или более линейно зависимые строки, получаемые из уравнений вида (9.2). Пусть для некоторых $\alpha_i \in F_2$, где $i = \overline{2,g}$, $g \in N$,

$$\sum_{k=1}^{l-h}\sum_{\{j_1^{(1)},j_2^{(1)},...,j_k^{(1)}\}\subset S^k_{I\setminus\{i_1^{(1)},i_2^{(1)},...,i_h^{(1)}\}}} a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)},j_2^{(1)},...,j_k^{(1)}\})} =$$

$$= \sum_{d=2}^{g}\alpha_d\sum_{k=1}^{l-h}\sum_{\{j_1^{(d)},j_2^{(d)},...,j_k^{(d)}\}\subset S^k_{I\setminus\{i_1^{(d)},i_2^{(d)},...,i_h^{(d)}\}}} a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)},j_1^{(d)},j_2^{(d)},...,j_k^{(d)}\})},$$

где $\{i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)}\} = \{i_1^{(d)},i_2^{(d)},...,i_h^{(d)}\}\setminus B$, $B = \{i_1,i_2,...,i_z\} = \bigcap_{i=1}^{g}\{i_1^{(d)},i_2^{(d)},...,i_h^{(d)}\}$.

Рассмотрим некоторый коэффициент из левой части равенства $a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)}\})}$. Так как $h<n$, то без нарушения общности

$$a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)}\})} = \sum_{d=2}^{g}\alpha_i a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)},j_1^{(d)}\})} \Leftrightarrow$$

$$\Leftrightarrow a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)}\})} = \sum_{d=2}^{2k+2} a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)},r_1^{(d)}\})},$$

где $2k+2 \le g$, $k \in Z_{\ge 0}$,

$$a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)}\})} = a_{\tau(\{_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)},r_1^{(d)}\})}.$$

Из предыдущих рассуждений следует

$$a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)},j_1^{(1)}\})} = a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)},r_1^{(d)}\})} \Leftrightarrow$$

$$\Leftrightarrow j_1^{(1)} \in \{i_{z+1}^{(d)},i_{z+2}^{(d)},...,i_h^{(d)}\},\ r_1^{(i)} \in \{i_{z+1}^{(1)},i_{z+2}^{(1)},...,i_h^{(1)}\},\ h = z+1.$$

Таким образом, верны равенства

$$a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(1)},i_{z+1}^{(d)}\})} = a_{\tau(\{i_1,i_2,...,i_z,i_{z+1}^{(d)},i_{z+1}^{(1)}\})},$$

где $i = \overline{1,2k+1}$. В проведенных рассуждениях элементы $j_1^{(1)}$ и $j_1^{(d)}$ выбраны произвольно, $d = \overline{2,2k+2}$, $h = l-1$. Таким образом, доказана следующая лемма.

Лемма 1. Линейно зависимые строки матрицы A системы уравнений вида (8), соответствующие уравнениям вида (9.2), при подстановке вектора $\bar{u}$ с l ненулевыми координатами $I = \{u_{i_1},u_{i_2},...,u_{i_l}\}$, где $1 \le i_1 < i_2 < ... < i_l \le n$, $1 \le l \le n$, имеют вид

$$a_{\tau(\{i_1',i_2',...,i_{l-1}',j\})} = b_{\tau(\{i_1',i_2',...,i_{l-1}'\})},$$

где $\{i_1',i_2',...,i_{l-1}'\} \subset S_I^{l-1}$; $I\setminus\{i_1',i_2',...,i_{l-1}'\} = \{j\}$. •

Теперь выделим линейно зависимые строки матрицы A системы уравнений вида (8) среди соответствующих уравнениям (9.4). Легко увидеть, что уравнения (9.2) отличаются от уравнений (9.4), наличием в последних среди фиксированных индексов свободного члена и неизвестных элементов, не принадлежащих множеству I номеров позиций ненулевых координат вектора $\bar{u}$, подставляемого в (8). Но суммирование в левой части обоих уравнений ведется по некоторому подмножеству I, которое является одинаковым для обоих видов уравнений (9.2) и (9.4). Таким образом, применяя рассуждения аналогичные рассуждениям для случая уравнений вида (9.2), можно убедиться, что верна

Лемма 2. Линейно зависимые строки матрицы A системы уравнений вида (8), соответствующие уравнениям вида (9.4), при подстановке $\bar{u}$ с l ненулевыми координатами $I = \{u_{i_1},u_{i_2},...,u_{i_l}\}$, где $1 \le i_1 < i_2 < ... < i_l \le n$, $1 \le l \le n$, имеют вид

$$a_{\tau(\{i_1',i_2',...,i_{l-1}',j_1',j_2',...,j_v',j\})} = b_{\tau(\{i_1',i_2',...,i_{l-1}',j_1',j_2',...,j_v'\})},$$

где $\{i_1',i_2',...,i_{l-1}'\} \subset S_I^{l-1}$, $I\setminus\{i_1',i_2',...,i_{l-1}'\} = \{j\}$, $\{j_1',j_2',...,j_v' \subset S^v_{[1..n]\setminus I}\}$, $1 \le v \le n-l$. •

Таким образом, в общем случае, когда $\overline{u}$ имеет l ненулевых координат $I=\{u_{i_1},u_{i_2},...,u_{i_l}\}$, где $1 \le i_1 < i_2 < ... < i_l \le n$, $1 \le l \le n$, из лемм 1 и 2, а также формул (9.1)–(9.4) следует, что множество «разрешенных» векторов $A_{i_1 i_2 ... i_l}$ состоит из векторов $\overline{y} \in F_2^{2^n}$, для коэффициентов которых выполняются следующие свойства:

1. $y_{\lambda(\tau(\{i_1,i_2,...,i_l,j_1^{'},j_2^{'},...,j_h^{'}\}))}=0$, $\forall\{j_1^{'},j_2^{'},...,j_h^{'}\}\subset 2^{[1..n]\setminus I}$, $h=\overline{1,n-l}$;

2. $y_{\lambda(\tau(\{i_1^{'},i_2^{'},...,i_{l-1}^{'}\}))}=y_{\lambda(\tau(\{i_1^{''},i_2^{''},...,i_{l-1}^{''}\}))}$: $\forall\{i_1^{'},i_2^{'},...,i_{l-1}^{'}\}$, $\{i_1^{''},i_2^{''},...,i_{l-1}^{''}\}\subset S_I^{l-1}$;

3. $y_{\lambda(\tau(\{i_1^{'},i_2^{'},...,i_{l-1}^{'},j_1^{'},j_2^{'},...,j_v^{'}\}))}=y_{\lambda(\tau(\{i_1^{''},i_2^{''},...,i_{l-1}^{''},j_1^{'},j_2^{'},...,j_v^{'}\}))}$: $\forall\{i_1^{'},i_2^{'},...,i_{l-1}^{'}\}$, $\{i_1^{''},i_2^{''},...,i_{l-1}^{''}\}\subset S_I^{l-1}$, при фиксированном $\{j_1^{'},j_2^{'},...,j_v^{'}\}\subset S_{[1..n]\setminus I}^{v}$, $1 \le v \le n-l$;

4. все элементы вектора $\overline{y} \in F_2^{2^n}$, не определенные свойствами 1–3, являются произвольными элементами поля F_2.

Теорема 2 (о существовании производной по направлению). Рассмотрим Φ_n. Пусть вектор $\overline{u} \in F_2^n$ содержит l ненулевых координат $I=\{u_{i_1},u_{i_2},...,u_{i_l}\}$, где $1 \le i_1 < i_2 < ... < i_l \le n$, $1 \le l \le n$. Положим, что $A_{i_1 i_2 ... i_l}$ — множество «разрешенных» векторов, определенных при подстановке в систему уравнений вида (8) вектора $\overline{u}$. Для булевой функции $g \in \Phi_n$ существует такая булева функция f, что

$$(D_{\overline{u}}f)(\overline{x})=g(\overline{x}) \Leftrightarrow \gamma(g)\in \bigcup_{i\in C_{[1..n]}} A_i ,$$

где γ — биекция (3); $C_{[1..n]}$ определено (5).

Доказательство. Докажем, что $\bigcup_{i\in C_{[1..n]}} A_i = Allowed$. Если это равенство верно, то утверждение теоремы будет выполняться в силу определения множества $Allowed$.

Очевидно, что в силу своего построения $\bigcup_{i\in C_{[1..n]}} A_i \subset Allowed$. Множество $A_{i_1 i_2 ... i_l}$ содержит все возможные вектора свободных членов $\overline{b}$, при которых система уравнений вида (8) совместна при подстановке вектора $\overline{u}$. Пусть $\overline{w} \in A_{i_1 i_2 ... i_l}$. При фиксировании $\overline{w}$ в качестве свободных членов системы (8) можно найти все возможные решения данной системы, которые определяют все булевы функции $f \in \Phi_n$: $D_{\overline{u}}f=\gamma^{-1}(\overline{w})$. Поскольку при построении множеств A_i, $i \in C_{[1..n]}$, перебираются все вектора $\overline{u} \in F_2^n$, кроме нулевого, то $Allowed \subset \bigcup_{i\in C_{[1..n]}} A_i$. •

Алгоритм определения существования прообраза. Представим в краткой форме алгоритм, позволяющий определить существование для данной булевой функции прообраза. На вход алгоритма поступает булева функция $g \in \Phi_n$ $(n>1)$, на выходе алгоритм выдает значение *true*, если прообраз для входной функции существует, иначе, при отсутствии прообраза, алгоритм возвращает значение *false*. Будем рассматривать алгоритм в виде двух частей, которые обозначим как алгоритмы А и Б. Алгоритм А определяет возможное направление, по которому была взята производная и отправляет его на вход алгоритма Б, который проверяет существует ли прообраз для булевой функции, поступившей на вход алгоритма с учетом выбранного направления.

Рассмотрим работу алгоритмов. На вход алгоритма А поступает вектор $\gamma(g)=(g_1,...,g_{2^n})\in F_2^{2^n}$. Выполняется проверка значения коэффициента g_{2^n}. Если этот коэффициент ненулевой, то согласно теореме 2 прообраза не существует, и алгоритм выдает *false*, иначе алгоритм продолжает работу. Далее алгоритм А формирует вектор $\overline{u}=(g_{2^n-1},g_{2^n-2},...,g_{2^n-n})\in F_2^n$, в направлении которого была предположительно взята производная, при условии, что $\overline{u}\ne\overline{0}$. Объяснение этого предположения легко видеть из (8). Если $\overline{u}\ne\overline{0}$, то происходит вызов алгоритма Б, работа которого описана ниже, иначе, если $\overline{u}=\overline{0}$, в цикле происходит последовательный перебор всех ненулевых векторов, принадлежащих F_2^n, которые подаются на вход алгоритма Б в качестве предполагаемого вектора, в направлении которого была взята производная. Если при выполнении алгоритма Б было установлено существование прообраза, то алгоритм А возвращает *true*.

Опишем работу алгоритма Б. На его вход которого поступают векторы $\gamma(g)\in F_2^{2^n}$ и $\overline{u}\in F_2^n$. Алгоритм Б проверяет выполняются ли для входного вектора $\gamma(g)$ необходимые и достаточные условия существования прообраза

по заданному направлению $\overline{u}$, то есть определяет принадлежность вектора $\gamma(g)$ множеству $A_{i_1 i_2 \dots i_l}$, где $i_1 i_2 \dots i_l \in C_{[1..n]}$, $W_{\overline{u}} = \{i_1, i_2, \dots, i_l\}$, множество $W_{\overline{u}}$ содержит номера ненулевых элементов вектора $\overline{u}$. Для поиска ответа алгоритм последовательно проверяет выполнение свойств 1-3 (см. список перед теоремой 2) для заданного входного вектора. Если входной вектор удовлетворяет всем трем свойствам, то, согласно теореме 2, можно утверждать, что для булевой функции, взаимно однозначно соответствующей данному вектору, существует прообраз в заданном направлении, и, следовательно, алгоритм Б возвращает значение *true*, иначе, при невыполнении хотя бы одного из условий, алгоритм возвращает *false*.

Авторами получена оценка временной сложности алгоритма $O(n+2^{3n})$. Доказательства оценки сложности данного алгоритма и других алгоритмов, представленных ниже, в данной работе не приводится в связи с их громоздкостью.

Пример.

Рассмотрим Φ_3. Пусть

$$\gamma(g(x_1,x_2,x_3)) = (g_1,g_2,g_3,g_4,g_5,g_6.g_7,g_8) = (1{,}1{,}0{,}1{,}0{,}0{,}0{,}0) \in F_2^{2^3},$$
$$g(x_1,x_2,x_3) = 1 + x_1 + x_3,$$

где $g(x_1,x_2,x_3) \in F_2[x_1,x_2,x_3]$.

Поскольку $g_8 = 0$, то пока нет оснований утверждать, что прообраза не существует. Рассмотрим вектор $\overline{u} = (g_7, g_6, g_5) = (0{,}0{,}0) \in F_2^3$. Следовательно, будем перебирать все ненулевые вектора F_2^3 в поисках подходящего направления. Упорядочим элементы F_2^3 следующим образом:

$$(0{,}0{,}0) < (1{,}0{,}0) < (0{,}1{,}0) < (0{,}0{,}1) < (1{,}1{,}0) < (1{,}0{,}1) < (0{,}1{,}1) < (1{,}1{,}1).$$

Пусть $\overline{u} = (1{,}0{,}0)$. Тогда $W_{\overline{u}} = \{1\}$, $2^{[1..3]\setminus W_{\overline{u}}} = \{\varnothing, \{2\}, \{3\}, \{2{,}3\}\}$. Очевидно, что $g_{\lambda(1)} = g_2 = 1$, то есть вектор $\overline{u}$ не удовлетворяет свойству 1 (см. список перед теоремой 2). Следовательно, алгоритм 1.2 возвращает значение *false*.

Пусть $\overline{u} = (0{,}1{,}0)$. Тогда $W_{\overline{u}} = \{2\}$, $2^{[1..3]\setminus W_{\overline{u}}} = \{\varnothing, \{1\}, \{3\}, \{1{,}3\}\}$. Вектор $\overline{u}$ удовлетворяет свойству 1: $g_{\lambda(2)} = g_3 = 0$, $g_{\lambda(12)} = g_5 = 0$, $g_{\lambda(23)} = g_7 = 0$ и $g_{\lambda(123)} = g_8 = 0$. Далее $S_3^0 = \{\varnothing\}$, то есть нет необходимости проверять выполняется ли свойство 2. Проверим выполнение свойства 3 для вектора $\overline{u}$. $S^1_{[1..3]\setminus W_{\overline{u}}} = \{\{1\}, \{3\}\}$, следовательно $g_{\lambda(1)} = g_2 = 1$, $g_{\lambda(3)} = g_4 = 1$. Далее $S^2_{[1..3]\setminus W_{\overline{u}}} = \{\{1{,}3\}\}$, следовательно $g_{\lambda(13)} = g_6 = 0$, то есть вектор $\overline{u}$ удовлетворяет свойству 3. Поскольку вектор $\overline{u}$ удовлетворил всем трем свойствам, то согласно теореме 2 для $g(x_1,x_2,x_3)$ существует прообраз. Следовательно, алгоритм А, а затем и алгоритм Б, выдает на выход значение *true*. •

Способ поиска интеграла булевой функции. Опишем еще один подход к решению задачи интегрирования булевых функций. Положим, что для фиксированного вектора при помощи алгоритма существования прообраза установлено, что решение существует. Легко увидеть, что при работе этого алгоритма находится вектор, в направлении которого взята производная. Таким образом, из теоремы 2 следует, что система уравнений вида (8) при подстановке в нее найденного вектора совместна и неопределенна. То есть можно построить общее решение [10] для этой системы, приняв в качестве неизвестных a_i, где $i \in C_{[1..n]}$, и выбрав в качестве неизвестного a_0 произвольный элемент поля F_2. Заметим, что a_i являются коэффициентами прообраза булевой функции, поступившей на вход алгоритма поиска прообраза. Можно использовать любой прямой метод для решения данной СЛАУ. К примеру, если использовать метод Гаусса [10], сложность которого равна $O(n^3)$, где n — количество неизвестных, встречающихся в системе, то можно показать, что асимптотическая оценка сложности решения задачи интегрирования булевой функции (с использованием метода Гаусса для решения СЛАУ) составляет $O(n+2^{3n}) + O(2^{3n}) = O(n+2^{3n})$. Авторами также установлено, что при использовании метода полного перебора для поиска прообраза, сложность решения задачи интегрирования булевой функции равна $O(2^{2^n+2n-2}(3n+10) + 2^{3n} + n)$. Таким образом, использование предложенных методов уменьшает алгоритмическую сложность поиска прообраза по сравнению с методом полного перебора примерно в $O(2^{2^n})$ раз.

Заключение. В работе получены существенные теоретические результаты, связанные с решением задач проверки существования и поиска прообраза для произвольной булевой функции, которая рассматривается как

значение производной по направлению. На основе полученных результатов построены соответствующие алгоритмы, проведена оценка их алгоритмической сложности. Выполненная работа может быть полезна для ряда разделов криптографии и теории кодирования, использующих булевы функции нескольких переменных.

Библиографический список

1. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. — Москва: МЦНМО, 2004. — 470 с.

2. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки. / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — Москва : Связь, 1979. — 744 с.

3. Сидельников, В. М. Теория кодирования / В. М. Сидельников. — Москва : ФИЗМАТЛИТ. — 2008. — 324 с.

4. Деундяк В. М. Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида-Маллера второго порядка / В. М. Деундяк, Н. С. Могилевская // Известия вузов. Сев.-Кав. регион. Техн. науки. — 2015.— №1(182). — С.3–10.

5. Могилевская, Н. С. Экспериментальное исследование декодеров кодов Рида-Маллера второго порядка / Н. С. Могилевская, В. Р. Скоробогат, В. С. Чудаков // Вестник Донского гос. тех. ун-та. — 2008. — Т.8, № 3. — С.231–237.

6. Могилевская, Н. С. Корректирующая способность декодера мягких решений троичных кодов Рида-Маллера второго порядка при большом числе ошибок / Н. С. Могилевская // Вестник Донского гос. тех. ун-та. — 2015. — № 1. — С.121–130.

7. Бохманн, Д. Двоичные динамические системы / Д. Бохманн, Х. Постхоф. — Москва : Энергоатомиздат, 1986. — 400 с.

8. Деундяк, В. М. Интегрируемость систем полиномов нескольких переменных первой и второй степени над простыми полями Галуа / В. М Деундяк, А. В. Кнутова // Известия ВУЗов. Северо-Кавказский регион. Естественные науки. — 2016. — №2. — С.41–46.

9. Алгоритм восстановления булевой функции по ее производной по направлению (электронный ресурс) / А. В. Мазуренко, Н. С. Могилевская // Системный анализ, управление и обработка информации: сб. трудов VI международного семинара. — Ростов-на-Дону, 2015. — Т. 1. — С.256–262. — Режим доступа : http://ntb.donstu.ru/content/2015421/ (дата обращения: 13.11.2016).

10. Глухов, М. М. Алгебра. Т. 1. / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — Москва : Гелиос АРВ, 2003. — 336 с.

References

1. Logachev, O.A., Salnikov, A.A., Yashchenko, V.V. Bulevy funktsii v teorii kodirovaniya i kriptologii. [Boolean functions in coding theory and cryptology.] Moscow: MTsNMO, 2004, 470 p. (in Russian).

2. McWilliams, F.J., Sloane, N.J.A. Teoriya kodov, ispravlyayushchikh oshibki. [The theory of error-correcting codes.] Moscow: Svyaz', 1979, 744 p. (in Russian).

3. Sidelnikov, V.M. Teoriya kodirovaniya. [Coding Theory.] Moscow: FIZMATLIT, 2008, 324 p. (in Russian).

4. Deundyak, V.M., Mogilevskaya, N.S. Model' troichnogo kanala peredachi dannykh s ispol'zovaniem dekodera myagkikh resheniy kodov Rida-Mallera vtorogo poryadka. [The model of the ternary communication channel with using the decoder of soft decision for Reed – Muller codes of the second order.] University News. North-Caucasian region. Technical Sciences Series, 2015, no. 1(182), pp. 3–10 (in Russian).

5. Mogilevskaya, N.S., Skorobogat, V.R., Chudakov, V.S. Eksperimental'noe issledovanie dekoderov kodov Rida-Mallera vtorogo poryadka. [Experimental research of second order Reed-Muller codes.] Vestnik of DSTU, 2008, vol. 8, no. 3, pp. 231–237 (in Russian).

6. Mogilevskaya, N.S. Korrektiruyushchaya sposobnost' dekodera myagkikh resheniy troichnykh kodov Rida-Mallera vtorogo poryadka pri bol'shom chisle oshibok. [Correcting capacity of soft-decision decoder of ternary Reed – Muller second-order codes with a large number of errors**.**] Vestnik of DSTU, 2015, no. 1, pp. 121–130 (in Russian).

7. Bohmann, D., Posthoff, Kh. Dvoichnye dinamicheskie sistemy. [Binary dynamic systems.] Moscow: Energoatomizdat, 1986, 400 p. (in Russian).

8. Deundyak, V.M., Knutova, A.V. Integriruemost' sistem polinomov neskol'kikh peremennykh pervoy i vtoroy stepeni nad prostymi polyami Galua. [Integrability of Systems of the First and Second Degree Polynomials of Several Variables over Simple Galois Fields.] Izvestiya vuzov. Severo-Kavkazskiy region. Natural Sciences. 2016, no. 2, pp. 41–46 (in Russian).

9. Mazurenko, A.V., Mogilevskaya, N.S. Algoritm vosstanovleniya bulevoy funktsii po ee proizvodnoy po napravleniyu. [Algorithm of Boolean function recovery from its directional derivative.] Sistemnyy analiz, upravlenie i obrabotka informatsii: sb. trudov VI mezhdunarodnogo seminara. [System analysis, information control and processing: Proc.

VI Int. Seminar.] Rostov-on-Don, 2015, vol. 1, pp. 256–262. Available at: http://ntb.donstu.ru/content/2015421/ (accessed: 13.11.2016) (in Russian).

10. Glukhov, M.M., Yelizarov, V.P., Nechaev, A.A. Algebra. T. 1. [Algebra. Vol.1.] Moscow: Gelios ARV, 2003, 336 p. (in Russian).

Поступила в редакцию 25.11.2016
Сдана в редакцию 25.11.2016
Запланирована в номер 11.01.2017

Об авторах:

Мазуренко Александр Вадимович, студент Донского государственного технического университета (РФ, 344000, г. Ростов-на-Дону, пл. Гагарина, 1), ORCID: http://orcid.org/ 0000-0001-9541-3374, mazurencoal@gmail.com

Могилевская Надежда Сергеевна, доцент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (РФ, 344000, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, ORCID: http://orcid.org/0000-0003-1357-5869, 79044430127@yandex.ru

Received 25.11.2016
Submitted 25.11.2016
Scheduled in the issue 11.01.2017

Authors:

Mazurenko, Alexander V., student, Don State Technical University (RF, Rostov-on-Don, Gagarin sq., 1), ORCID: http://orcid.org/ 0000-0001-9541-3374, mazurencoal@gmail.com

Mogilevskaya, Nadezhda S., associate professor of the Cybersecurity of IT Systems Department, Don State Technical University (RF, Rostov-on-Don, Gagarin sq., 1), Cand. Sci. (Eng.), ORCID: http://orcid.org/0000-0003-1357-5869, 79044430127@yandex.ru